



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| | | | | |
|--|-------------|----------------------|--------------------------------|------------------|
| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
| 10/043,910 | 01/11/2002 | Frank Lee | TRNDP006 | 7252 |
| 58766 | 7590 | 07/09/2008 | | |
| Beyer Law Group LLP P.O. BOX 1687 Cupertino, CA 95015-1687 | | | EXAMINER MOORTHY, ARAVIND K | |
| | | | ART UNIT | PAPER NUMBER |
| | | | 2131 | |
| | | | NOTIFICATION DATE | DELIVERY MODE |
| | | | 07/09/2008 | ELECTRONIC |

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

SBEYER@BEYERLAW.COM
ldean@beyerlaw.com

| | | | |
|------------------------------|---------------------------------------|-----------------------------------|--|
| Office Action Summary | Application No. 10/043,910 | Applicant(s) LEE ET AL. | |
| | Examiner Aravind K. Moorthy | Art Unit 2131 | |

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 20 June 2008.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-8, 10-17, 21-25 and 36-38 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-8, 10-17, 21-25 and 36-38 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 11 February 2002 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☒ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This is in response to the communications filed on 20 June 2008.
2. Claims 1-8, 10-17, 21-25 and 36-38 are pending in the application.
3. Claims 1-8, 10-17, 21-25 and 36-38 have been rejected.
4. Claims 9, 18-20 and 26-35 have been cancelled.

Response to Arguments

5. Applicant's arguments with respect to claims 1-8, 10-17, 21-25 and 36-38 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 1-8, 10-17, 21-25 and 36-38 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Independent claims 1 and 16 have been amended to recite "a proxy module that modifies the request for content by adding a redirection destination header to the request so that it is redirected to a proxy server if the protocol is only for requesting and retrieving content". The examiner understands that the request is going to be redirected if it is of protocol for requesting and retrieving content. However, it is unclear to the examiner what happens to the packet if the request is not of protocol for requesting and retrieving content. The examiner is unclear if the request is dropped, rejected or blocked. Clarification is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1-7, 10-17, 19-25 and 36-38 are rejected under 35 U.S.C. 102(e) as being anticipated by Taylor et al U.S. Patent No. 6,728,885 B1 (hereinafter Taylor).

As to claim 1, Taylor discloses a system for identifying undesirable content in responses sent in reply to a user request for content, the system comprising:

a user input device that generates a request for content including an address of a target server and a protocol field (i.e. For instance, a plurality of packets from the outside networks arrives at NIC 203. Each received packet is examined separately by firewall 201. More specifically, when a packet is received by NIC 203 from any one of outside networks 111, 115, the packet is associated with a corresponding port number. The packet is, then, forwarded to NAT 205 which translates the destination address of the received packet into a corresponding address of internal hosts. The packet is then sent to DPF 207 for further examination and processing) [column 5, lines 28-38];

a network component that executes a redirection program, the redirecting program including a scan module that receives the user request

for content before the request is processed for transmission to the target server and is capable of identifying the request as a request for content by scanning the protocol field and identifying a protocol that is only for requesting and retrieving content (i.e. Each entry in the user specified static filter rules includes the attributes discussed above and a value indicating the type of filter to apply to the packet. The types of filters include "permit" filter to forward the packet to its destination, "deny" to discard the packet, "absorb" to apply an application level filter and "a filter all rule" discussed above. In order to provide a finer granularity in the packet filtering)[column 11, lines 12-19], and a proxy module that modifies the request for content by adding a redirection destination header to the request so that it is redirected to a proxy server if the protocol is only for requesting and retrieving content (i.e. For incoming packets, if the packet was part of a connection, i.e., not a SYN packet, if it was to be forwarded to firewall 201 and if transparency is OFF on the port on which it was received, then the packet's destination address is modified with the real destination, i.e., the address of an internal host computer which the packet is to be sent. It is an error if transparency is ON and the packet's destination address was not firewall 201 and there was no user specified filter rule matching the packet) [column 11, lines 59-67];

a network that routes the request for content to the proxy server (i.e. Now referring to the transparency procedure in step 401 of FIG. 6, DPF 207 determines if the transparency for the port on which the packet

Art Unit: 2131

was received is on. If the transparency is on, the packet is sent to TPF 215.

In this case, the packet is eventually forwarded to proxy 211 to be filtered at the application layer level. If the transparency is off, the packet is sent to its destination. For instance, if the destination is firewall 201, the packet is sent to proxy 211; and if the destination is an internal host computer, the packet is sent to the internal host) [column 11, lines 43-52]; and

the proxy server that receives user-defined configuration data during a negotiation phase of establishing a connection between the proxy module and proxy server, receives the request for content, removes the redirection header, forwards the request to the target server, and receives a response from the target server [column 11, lines 59-67], the proxy server having a decoding module for decoding the response a content scanning module to scan a decoded response and a user-defined configuration data scanning module to apply user-defined configuration data to the decoded response and a return address appending module [column 12, lines 5-19].

As to claim 2, Taylor discloses that the proxy server identifies undesirable content in the response and processes the response according to defined parameters [column 11, lines 59-67].

As to claim 3, Taylor discloses that the proxy server sends at least a portion of the response to the user, the portion of the response not including the undesirable content [column 12, lines 30-45].

Art Unit: 2131

As to claim 4, Taylor discloses that the proxy server sends a notification message back to the user, the notification message containing data related to the undesirable content [column 12, lines 30-45].

As to claim 5, Taylor discloses the system further comprising:

a user preference module that receives user-defined parameters utilized by the proxy server when processing the response [column 6, lines 44-57].

As to claims 6 and 19, Taylor discloses that the proxy module redirects the request to the proxy server by modifying the request [column 11, lines 43-52].

As to claims 7 and 20, Taylor discloses that the proxy module modifies the request by adding a redirection destination header to the request [column 11, lines 43-52].

As to claim 10, Taylor discloses that the defined parameters are proxy server default parameters [column 6, lines 44-57].

As to claim 11, Taylor discloses that the defined parameters are user-defined parameters [column 6, lines 44-57].

As to claim 12, Taylor discloses that the defined parameters are a combination of userdefined parameters and proxy server default parameters [column 6, lines 44-57].

As to claims 13 and 14, Taylor discloses that the scan module and the proxy module are located in a network gateway device [column 11, lines 12-19].

As to claim 15, Taylor discloses that the network gateway device further comprises a firewall and a router [column 11, lines 12-19].

As to claim 16, Taylor discloses a method for identifying undesirable content in responses sent in reply to a user request for content, the method comprising:

receiving, at a redirection program executing on a network computing device, input from a user computer including at least one request for content addressed to a target server, the request having an address of the target server and a protocol field (i.e. For instance, a plurality of packets from the outside networks arrives at NIC 203. Each received packet is examined separately by firewall 201. More specifically, when a packet is received by NIC 203 from any one of outside networks 111, 115, the packet is associated with a corresponding port number. The packet is, then, forwarded to NAT 205 which translates the destination address of the received packet into a corresponding address of internal hosts. The packet is then sent to DPF 207 for further examination and processing) [column 5, lines 28-38];

before the request is transmitted on a network, scanning at a scan module in the redirection program the protocol field of the request for content to determine whether a protocol of the request is only for requesting and retrieving content (i.e. Each entry in the user specified static filter rules includes the attributes discussed above and a value indicating the type of filter to apply to the packet. The types of filters include "permit" filter to forward the packet to its destination, "deny" to discard the packet, "absorb" to apply an application level filter and "a filter

all rule" discussed above. In order to provide a finer granularity in the packet filtering)[column 11, lines 12-19];

at a proxy module in the redirection program, modifying the request by adding a redirection header to the request, thereby redirecting the request to a proxy server (i.e. For incoming packets, if the packet was part of a connection, i.e., not a SYN packet, if it was to be forwarded to firewall 201 and if transparency is OFF on the port on which it was received, then the packet's destination address is modified with the real destination, i.e., the address of an internal host computer which the packet is to be sent. It is an error if transparency is ON and the packet's destination address was not firewall 201 and there was no user specified filter rule matching the packet) [column 11, lines 59-67];

receiving the request for content at the proxy server [column 11, lines 59-67];

receiving user-defined configuration data at the proxy server during a negotiation phase of establishing a connection between the proxy module and proxy server [column 11, lines 59-67];

removing the redirection destination header from the request at the proxy server [column 12, lines 5-19];

sending the request for content from the proxy server to the target server for generation of a response [column 12, lines 5-19];

receiving the response from the target server at the proxy server [column 12, lines 5-19];

Art Unit: 2131

decoding the response at the proxy server [column 12, lines 5-19];

scanning the decoded response for a computer virus, junk e-mail, or pornographic content at the proxy server [column 12, lines 30-45];

if a computer virus, junk e-mail or pornographic content is detected, processing the decode response at the proxy server according to the user-defined configuration data, re-encoding the response and appending a return address so that the response is sent to the user computer [column 12, lines 30-45]; and

if a computer virus, junk e-mail, or pornographic content is not detected, re-encoding the response and appending the return address so that the response is sent to the user computer [column 12, lines 30-45].

As to claim 17, Taylor discloses the method further comprising:

identifying undesirable content in the response [column 12, lines 30-45];

modifying the response to remove the undesirable content [column 12, lines 30-45]; and

sending the modified response from the proxy server to the user computer [column 12, lines 30-45].

As to claim 21, Taylor discloses that the request for content is redirected to the proxy server by establishing a session with the proxy server [column 9, lines 17-26].

As to claim 22, Taylor discloses the method further comprising:

receiving input of at least one user-defined parameter at the proxy module which stores the parameter in a database and may forward to the proxy server during negotiation phase of the connection with the proxy server [column 6, lines 44-57].

As to claims 23, Taylor discloses that the user-defined parameter is input using a browser application [column 6, lines 44-57].

As to claim 24, Taylor discloses that the user-defined parameter is sent to the proxy server by modifying the request for content [column 6, lines 44-57].

As to claim 25, Taylor discloses that the user-defined parameter is sent to the proxy server during a session established with the proxy server [column 6, lines 44-57].

As to claim 36, Taylor discloses storing the user-defined configuration data at the proxy module [column 6, lines 44-57].

As to claim 37, Taylor discloses storing the user-defined configuration data at the proxy server [column 6, lines 44-57].

As to claim 38, Taylor discloses retrieving the previously stored user-defined configuration data at the proxy server when processing the decoded response [column 6, lines 44-57].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

8. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Taylor U.S. Patent No. 6,728,885 B1 as applied to claim 1 above, and further in view of Smithson et al US 6,898,715 B1.

As to claim 8, Taylor does not teach that the proxy server further quarantines undesirable content.

Smithson et al teaches a proxy that quarantines computer virus outbreaks [column 6 line 13 to column 7 line 17].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Taylor so that the proxy server would have quarantined undesirable content it was content containing a virus.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Taylor by the teaching of Smithson et al because it prevents the undesirable content (i.e. virus) to spread throughout the network [column 1, lines 48-64].

Conclusion

9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2131

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Aravind K Moorthy/

Examiner, Art Unit 2131

/Ayaz R. Sheikh/

Supervisory Patent Examiner, Art Unit 2131